Identity, advertising, and algorithmic targeting: or how (not) to target your "ideal user"

Article (Published Version)

null • Summer 2021

Identity, Advertising, and Algorithmic Targeting: Or How (Not) to Target Your "Ideal User"

Tanya Kant[1]

[1]**Media and Cultural Studies, University of Sussex, UK**

Published on: Aug 10, 2021

ABSTRACT

Targeted or "personalized" marketing is an everyday part of most web users' experience. But how do companies "personalize" commercial web content in the context of mass data aggregation? What does it really mean to use data to target web users by their "personal interests" and individual identities? What kinds of ethical implications arise from such practices? This case study explores commercial algorithmic profiling, targeting, and advertising systems, considering the extent to which such systems can be ethical. To do so the case study first maps a brief history of the commercially targeted user, then explores how web users themselves perceive targeted advertising in relation to data knowledge, cookie consent, and "algorithmic disillusionment." It goes on to analyze current regulatory landscapes and consider how developers who target audiences might avoid placing burdens of impossible data choice on web users themselves. Finally, it offers a series of reflections on best practice in terms of how (not) to profile and target web users. To illuminate the ethical considerations connected to commercial targeted advertising systems, this case study presents some study tasks (see Exercises 1 and 2) that can be used as discussion points for those interested in exploring the nuances of targeting in specific contexts.

Keywords: targeting, advertising, algorithms, identity, profiling

Tanya Kant
Media and Cultural Studies, University of Sussex, UK

Introduction

Targeted profiling and marketing are common parts of users' daily web experiences: most people will have encountered "personalized" news feeds, individually recommended content, customized advertising, and tailored "sponsored stories." In most instances, algorithmic profiling is key to targeting: users' behaviors, click-throughs, inferred identity markers, and other signals must be profiled and categorized in order to establish what is of "personal relevance." Targeting mechanisms use a dizzyingly extensive list of categories to profile people: gender, age, ethnicity, lifestyle and consumption preferences, language, voice recordings, facial recognition, location, political leanings, music and film taste, income, credit status, employment status, home ownership status, marital status—the list goes on. These profiles are made useful and profitable through establishing "like-to-like users" who

are aggregated with and against other groups of users.

Though framed as a user-facing benefit by platforms, targeted content is not primarily the goodwill gesture it might first appear: instead, the user data mined as part of targeting processes function as *the* driving economic resource for the contemporary free-to-use web. As a market model this data-for-services exchange is extremely successful: in 2020 the world's biggest data tracker, Facebook, made $31.43 billion in ad revenue in the United States alone.[1] It is not an overstatement to propose that user targeting underpins the online economy as we know it.

Of course, there are benefits to having services algorithmically rendered "more relevant": cookies streamline site visits by storing user details, autofilling technologies can quickly complete registration forms, and filtering systems manage otherwise unmanageable amounts of content, all while the data needed for such user benefits is doubly harnessed to make platform profits. Despite (or indeed because of) its monetizable qualities, targeting creates a host of stark ethical problems in relation to identity articulation, collective privacy, data bias, raced and gendered discrimination and socioeconomic inequality. John Cheney-Lippold argues that computationally categorizing users as "male," "female," "high cost," "celebrity," and so on works to reductively produce, govern, and (re)shape selfhood.[2] As Caroline Bassett puts it, "digital interpellation can reduce life to a single line in a database entry: refugee, security threat, postcode offender, visa over-stayer, bad credit risk" in ways unknown to the users interpellated.[3] It's not just individualistic selves who are managed, reduced, and verified through data—as critiques such as T. L. Taylor's highlight, collective audiences are also reduced and reshaped through algorithmic sorting and auditing techniques.[4]

Algorithmic targeting might be about *predicting or anticipating* the needs and behaviors of individuals and audiences, but such anticipations have very material affects. Beverley Skeggs has found that bids are made by advertisers for access to Facebook users' data on average fifty million times a day in ways that create a kind of data underclass who are then exploited by credit lenders.[5] Safiya Noble finds racist categorization practices inherent in Google Search's collaborative data sets.[6] Cathy O'Neil argues that users' data are used to predict and manage users' future and present socioeconomic positionalities, often with detrimental consequences.[7] Targeting systems do not just match the "right" products with the "right" consumers—

they can discriminate, govern, and regulate web users in ways that demand close attention to ethical targeting practices.

A History of the Data-Tracked User

The following section outlines a partial history of the data-tracked user.[8] For this brief case study, this timeline includes developments in *commercial* targeting rather than developments in algorithmic policing, spatial infrastructures, medicine, and education, all of which are related but deserve their own timelines.[9]

Visit the web version of this article to view interactive content.

1940s. "Identity scoring" emerges: the categorization of individuals to calculate the benefits or risks of lending credit to certain groups of people.

1969. The US Defense Advanced Research Projects Agency (DARPA) military initiative produces the first iteration of the internet. Its development is driven by "a multitude of actors," some of which are commercial and interested in the internet's implementation outside of military use.[10]

1970-80s. "Niche marketing" is developed in satellite TV and magazine industries, which segments audiences to sell more lucrative advertising slots.

1980s. The internet becomes increasingly privatized by internet service providers (ISPs) who use commercial enterprises to make the internet widely available.

1991. The World Wide Web is created.[11] It is celebrated by proponents such as Howard Rheingold as a noncommercial space that exists for the common good.[12]

1993–1997. Business actors urge the commercialization of some elements of the web. Bill Gates (1995) sees potential in online services to automatically suggest personally relevant content, and John Hagel and Arthur Armstrong (1997) envisage a web where user preferences can be monitored to create customized recommendations.[13]

1994. AT&T displays the first ever banner ad on HotWired (now Wired). The development of the "click-through" model allows advertisers to see when an (anonymously defined) user has clicked on their advertisement.

1994. The HTTP cookie is developed.[14] In its development stages, web users could fully restrict what data cookies could collect. However, data privacy measures were quickly removed, and users lost the power to control cookie data before the technology became widespread.[15]

Mid-1990s. Online advertising becomes more prevalent, but most companies struggle to successfully monetize online media consumption.[16]

1996. Ad networks (platforms that serve as brokers between groups of publishers and groups of advertisers) increasingly emerge, including Doubleclick (now owned by Google).

1997. Developer / commentator Ethan Zuckerman hails algorithmic analyses of web page content as a new way to demographically target and monetize web users.[17] He argues, however, that this form of revenue generation is built on investor speculation rather than data accuracy.

1998. Open Profiling Standard (OPS) is bought and rolled out by Microsoft. OPS could securely store and manage individuals' personal information and credit card details, allowing user profiles to be exchanged between vendors.

2000-2003. Online revenue through advertising actively falls, as "banner ads" fail to compete with TV and print advertising.

2003. Ad networks such as AdSense begin to be adopted, allowing for automated matching of website content to advertising content. This allowed small web publishers to easily sell ad space.

2006. Popular ad-blocking software, AdBlock Plus, launches.

Mid-2000s. Real-time bidding is developed, which allows advertisers to bid in real time for ad space.[18]

2008. Behavioral targeting begins to be integrated into real-time bidding, marking a crucial shift away from *media content* toward *user behavior* as key to targeting.

2010. Attorney Joseph H. Malley creates the term "zombie cookies" to describe HTTP cookies that are recreated after deletion. These are just one form of cookies designed to be "almost impossible to circumvent": other variations include "supercookies," "ubercookies," and "evercookies."[19]

2011. Facebook launches its third-party app system, allowing apps such as Spotify and Candy Crush to collect large amounts of personal data about Facebook users and users' friends.

2013. Edward Snowden reveals that commercial platforms such as Google and Facebook have been aiding the state "dataveillance" of millions of web users in the United States and the United Kingdom.

2013. Nick Nikiforakis *et al.* find that commercial data trackers have a range of "cookieless" methods for identifying and anticipating users, including Flash and canvas fingerprinting, which cannot be easily deleted or detected.[20]

2014. The World Wide Web Foundation/ Sir Tim Berners-Lee launch The Web We Want campaign, which among other things calls for a return to Berners-Lee's original vision of a noncommercial and public web.

2014. In response to public outcries about data harvesting, Facebook imposes a ban on data collection by apps. Facebook promises to rollout "Anonymous Login" that will allow users to access apps without sharing any data.[21] However, the ban is soon lifted, and Anonymous Login is never introduced.

2018. Analytics company Cambridge Analytica is found to be exploiting targeting systems that can "target voters with personalised political advertisements," sparking debates that personalized political advertising is unduly influencing elections.[22]

2018. The European Union (EU) rolls out the General Data Protection Regulation (GDPR) legislation, intended to give EU citizens more security over personal data. However, legal loopholes such as "legitimate interest" allow for collection of otherwise GDPR-protected personal data.

2019. Following a series of lawsuits around discriminatory targeting, Facebook introduces a new nondiscrimination advertising policy. This includes a blanket targeting ban to advertisers in the housing, employment, and credit markets.

2020. The EU proposes a new Digital Services Act, designed among other things to restrict the use of personal data for targeted advertising purposes.

2020. Apple bans third-party cookies and Google pledges to do so by 2022, prompting debates on the so-called "cookie apocalypse." Though welcomed by privacy-concerned users, third-party marketing companies such as Criteo experience a fall in share values

and argue that the erasure of third-party cookies gives even more power to monopolistic first-party data trackers.[23]

Exercise 1: Feminist, Nerd, Alcoholic? Meeting Your "Algorithmic Self"

Google and Facebook claim to give their users insight into how they are profiled through "Ad Preferences" pages that allow users to see their explicitly and implicitly inferred demographics and interests. If I go on my Facebook ad preferences, I can see my inferred "interests" include "bourbon whiskey," "fire," "goat," "nerd," "gender," "boredom"; Google has me interested in "baked goods," "babies and toddlers," and "banking" (see Figure 1) among other things. These are glimpses of what Kyle Jarrett and John Cheney-Lippold call our "algorithmic identities."[24]

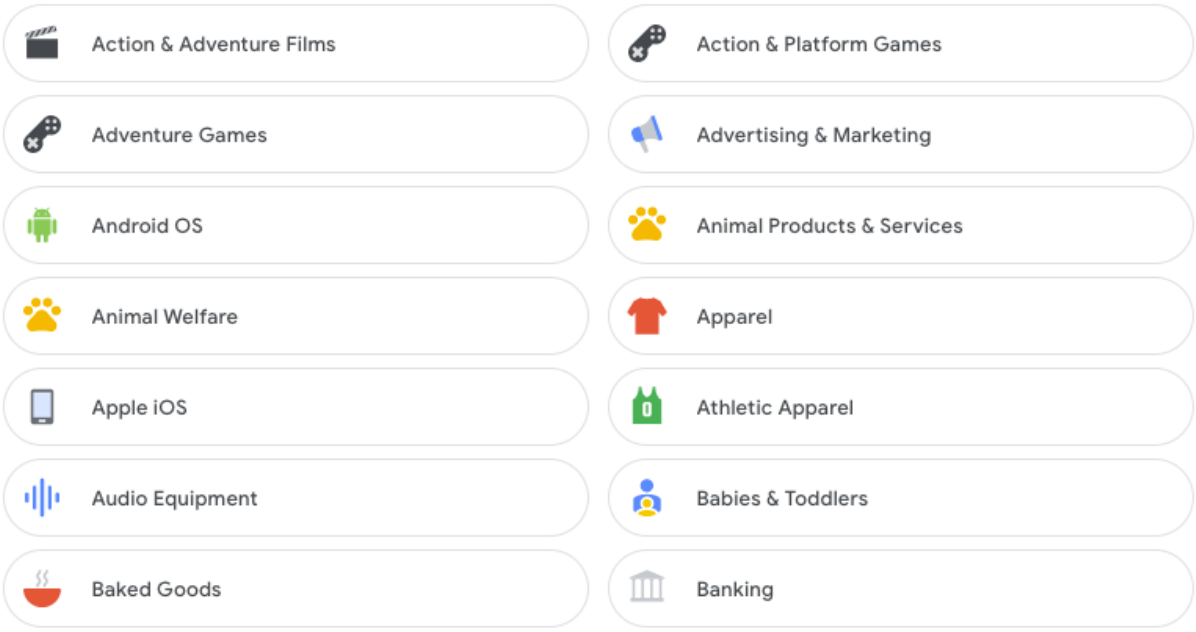

Figure 1. A selection of the author's "Google Ad Preferences."

Access your "Ad Settings" Profile on Google, Facebook or Instagram. Or if you regularly use another platform, try finding out if they have ad settings and if you can access them.

Questions for discussion:

- What does your "algorithmic identity" look like? Does it reflect your demographics and interests?
- How much do these Ad Preference profiles really tell us about algorithmic targeting? Do you feel like you know more about targeting processes after looking at your preferences?
- These interest categories change frequently and are recursive: an ad interest you are associated with can determine what ad interest you'll be categorized with next. What can this tell us about profiling?
- Do you agree with scholars such as Cheney-Lippold and Bassett that there is an overreduction of identity here? Why is this an ethical concern?

- Ethically, does it matter more if these profiles get your interests "right" or "wrong"?
- Does your gender and race play a part in how you are labelled? What are the ethical implications of this?

Audience Perceptions: Consent, Awareness, and Algorithmic Disillusionment

As little as a decade ago it was commonly perceived that most web users didn't know they were tracked and profiled. However, in the wake of the Snowden and Cambridge Analytica scandals, public awareness of tracking has grown substantially.[25] Yet beyond the fact that people are "aware" of tracking, the nuances of what this means for those targeted are complex and at times contradictory, and therefore demand ethical reflection.

Though cookie notices are frequently noticed by users, Ofcom has reported that 53 percent of UK web users never click on them and 65 percent of users do not read website terms and conditions before accepting them.[26] According to Ofcom and Joseph Turow and collaborators, this acceptance does not mean individuals are "happy" with being tracked: instead, users feel "resigned" to tracking that is so ubiquitous as to be unavoidable.[27] This is reflected in the continued use of tracker-blocking software, which is frequently used by around 25 percent of web users in the United Kingdom and United States. A similar proportion use ad-blocking software, suggesting that it is not just privacy that bothers people but the invasive presence of ads on their daily experiences of the web.

Furthermore, though people are aware they are being tracked, they do not know the specifics of who is tracking them, when, and why. For example, Ofcom found that 44 percent of users who reported being "confident in managing their personal data" were unaware that smartphone apps could collect personal data.[28] My own work suggests levels of expertise also play a role in user perceptions, though not in the way we might first expect. In a study of sixteen privacy-concerned web users, I found that those who might be termed "power users"—web users with high amounts of technical expertise and literacy—were actually *more likely* to feel anxious about targeting than those users who were less technologically skilled.[29] As study participant and machine learning researcher Robkifi put it:

> The odd thing is that I work in this field so I'm fairly well aware of what's out there, but I don't have the feeling I'm on top of it, and I find that very, that bothers

> me and [online privacy tools] probably give you a false sense of security that you are on top of it.[30]

Contrary to the idea that (data) knowledge is power, it seems the more you know about data tracking, the less you feel you can "stay on top" of your own data trail. Thus, ethical data tracking isn't simply about informing users that they are being tracked: users need to know how and, most importantly, *why* platforms track them, in ways that account for both present and future uses of targeting data.

There is a wide amount of variation in the types of targeting that people find acceptable and the types they do not. The *Guardian* has suggested that people are most unhappy with targeted political advertising.[31] However, targeting is not always perceived as negative: Ofcom has found that many people are happy with data collection if they receive appropriate reassurance about the protection and use of their data.[32] They also found that in the United Kingdom, 54 percent of web users would rather see relevant ads than "nonrelevant" ads: relevance being an ambiguous term here, as explored below. My own work suggests that being identified correctly by profiling systems can bring a sense of legitimacy and stability to some users' identities. For example, in a study with Google mobile assistant users, I found that some users—such as UK student Rachel—found their Google Ad Preferences profile to be pleasing:

> Oh, it does know I'm female! That's nice! Oh, and I have got interests! I've got so many interests! . . . I've got so many good ones! I've got like loads of animal ones, like dogs, wildlife, which I'm super into. I've got like five out of 65 that I don't do, but the rest of them are pretty good. … I'm quite happy now, at least it knows my interests.[33]

It seems there can be a pleasure in being algorithmically "recognized" by platforms; yet this pleasure emerges less out of platform capabilities in themselves, and more because users *assume personal relevance* in targeted technologies or content.[34] Others have found that audiences tend to *overstate* algorithms' predictive qualities in ways that far outstrip the capabilities of decision-making algorithms and recommenders.[35] When the material capabilities of algorithmic profiling *are* revealed to users, Aurelia Tamò Larrieux and collaborators find a kind of "algorithmic disillusionment" at work in user responses, wherein users are underwhelmed to find that profiling systems are often inaccurate or work via crude systems of inference.[36] This begs the question: will the problem of algorithmic disillusionment lessen as targeting systems become more technologically advanced? If so, does the algorithmic

power that would come with such advancements further entrench matters of marginalization, privacy invasion, and user powerlessness? It seems there is an ethical question of balance between predictive performance and user control that is required if developers are to dispel users' myths without affording too much predictive power to targeting systems.

So how do we empower users when it comes to data profiling? It seems flawed to keep giving users detailed knowledge or control mechanisms via legal privacy documents: the reception of the EU GDPR law suggests that the public feels overwhelmed by the endless requests for consent the law creates.[37] In being positioned as individually responsible for their own data trails, users are asked to take on the burden of knowing and consenting to platforms' often unknowable data management practices. Ethically, the individual and collective harms of this burden are considerable: the same data sets can and have been used to wrongly profile, exploit and marginalize users or groups of users, even when "consent" has been given (see Exercise 2 for more). Monica Henderson and colleagues suggest instead that users need to be taught "algorithmic literacy": education in artificial intelligence (AI)-driven processes that can further the public's understanding of algorithmic power.[38] Algorithmic literacy looks to dispel the algorithmic disillusionment of finding that algorithms do not always get things "right." It allows users to see algorithms as something that they can tactically work with or against, facilitating better critical decisions not just about specific cookie notices but the wider algorithmic landscape.

Exercise 2: Targeting Advertising as Raced and Gendered Discrimination

As well as the implications for election influencing that the Cambridge Analytica scandal highlighted, the "everyday" tracking practices behind personalized marketing are also intertwined with issues of raced and gendered discrimination. For example, in 2019 the US National Fair Housing Alliance sued Facebook for providing an option for "advertisers to exclude families with children and women from receiving advertisements, as well as users with interests based on disability and national origin" without Facebook's users' knowledge.[39] In 2018, the American Civil Liberties Union (ACLU) and ProPublica found employers advertising for jobs such as taxi drivers, roofers, and housing removals were permitted by Facebook's systems to be seen by only male users (see Figure 2). As a consequence of such legal action, Facebook has paid out millions of dollars in settlements.

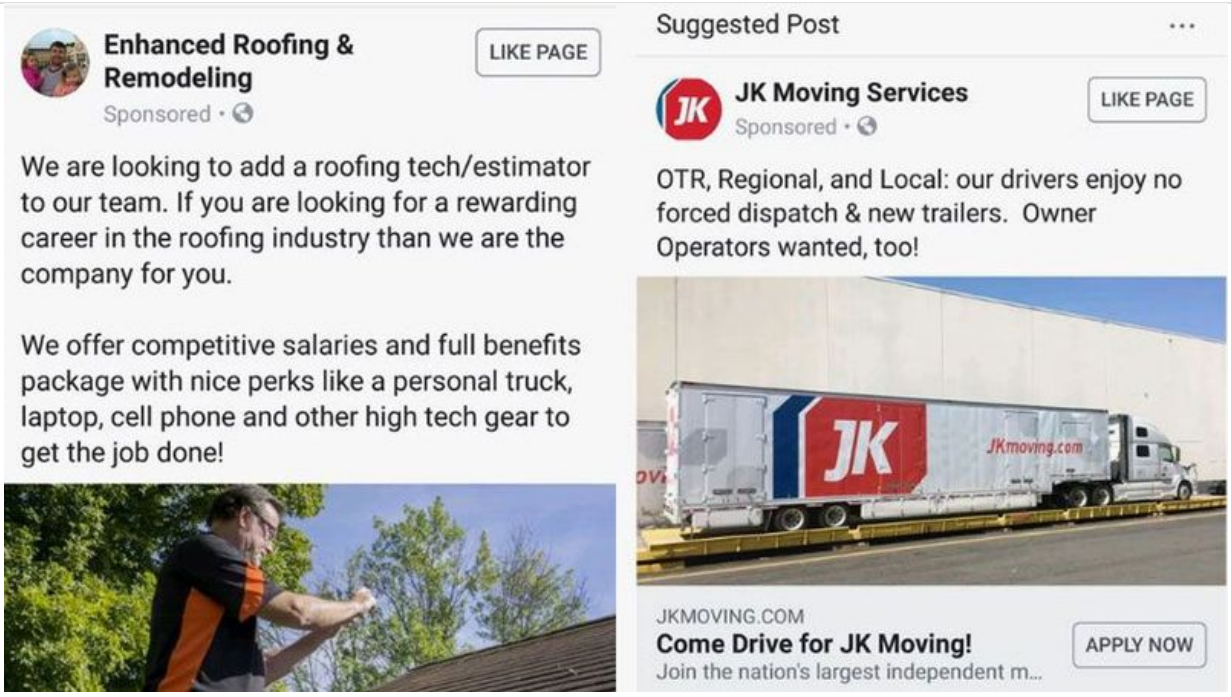

Figure 2. Examples of the Facebook ads for jobs targeted exclusively to computationally categorized "male" users. Source: https://www.bbc.co.uk/news/technology-45569227

Questions for discussion:

- Who should police these guidelines: Governments? International agencies? Users themselves?
- Should we allow the everyday tracking of users for personalized marketing when the short-term benefits of individual relevance come at such a large price for some groups?
- Do you feel marginalized or stereotyped by the targeted ads you see online? What part does your race, age, gender, or other identity positions play in this?

Database Ethics: Targeting from Platform Perspectives

In the last few years there has been increased public and policy pressure to ensure data targeting is enacted by platforms in responsible ways. In 2019 Facebook introduced a new nondiscrimination policy that disallows the use of their audience-selection tools to "wrongfully target" specific groups or "wrongfully exclude" certain groups from seeing ad content. Similarly, Google doesn't allow personalized advertising based on a user's fundamental or intrinsic self-identity, belief systems, or personal hardships, and appeals against using overly narrow or specific audiences. The company has also announced a move away from "individualized targeting" toward

"group targeting" and has introduced stricter political advertising rules that restrict microtargeting.[40]

What exactly does "wrongful targeting" mean here? Targeting inherently involves classifying and distinguishing audiences, so in some ways all forms of targeting can be considered exclusionary. As Clemens Apprich and coauthors argue, in computer science "pattern discrimination" is seen as a technically neutral term that describes the imposition of identifiers on input data in order to filter (i.e., to discriminate) information.[41] However, they emphasize that "far from being a neutral process, the delineation and application of patterns is in itself a highly political issue, even if hidden behind a technical terminology."[42] Audience targeting is therefore hard-coded for discrimination, and as a result, Wendy Chun appeals for computational systems that *actively challenge* existing sociocultural and economic inequalities. She asks computer scientists to devise systems that "displace the disturbing eugenic and segregationist histories that haunt our current network structures," using predictive models not as guides but as tools to detect oppressive pattern discriminations.[43]

Others such as Safiya Noble point out that the "ideal user" developers may imagine is constructed in ways that reinforce assumptions that the "average user" is white, cis-gendered male, middle class, and heterosexual.[44] Researchers such as Elizabeth Van Couvering, Eli Pariser, and Malte Ludewig and colleagues ask that developers not take the concept of "personal relevance" at face value: they suggest that democratic engagement, opposing points of view, coverage, diversity, and novelty (among other factors) should be considered to avoid insular and detrimentally myopic forms of web consumption.[45] However, being too "personally relevant" is not the only problem: being too broad can also lead to ethical issues. For example, Elizabeth Reed and I have described how fertility-based targeting on Facebook seems to assume that those gendered as "women" will automatically be interested in egg freezing or ovulation tests (see Figure 3).[46] This is largely because, as Rena Bivens and Oliver Haimson note, Facebook's algorithmic marketing system constructs gender as resolutely "male" or "female."[47] They find that "despite the wealth of other behavioral and taste-based data available now," this binary offers to advertisers two large and profitable groups constructed entirely through gender.[48] Thus, such blanket-targeting works on the essentialist and conservative assumptions that algorithmically categorized women are both fertile and interested in producing children.

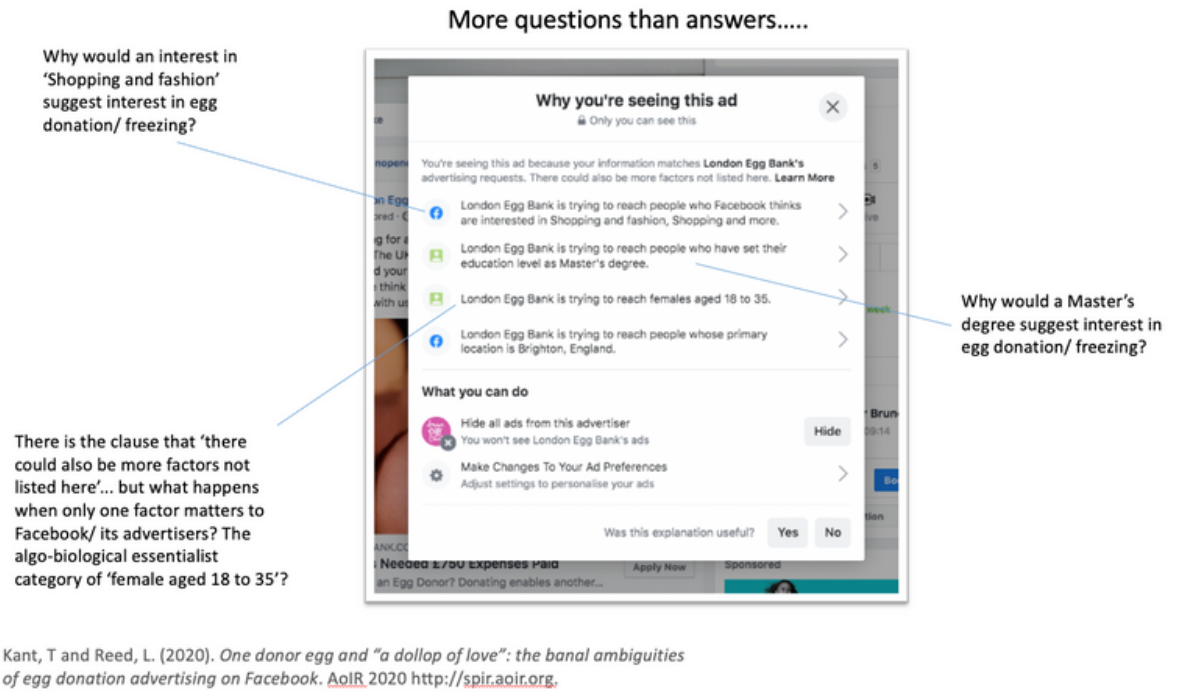

Figure 3. Annotated screenshot of Facebook's explanation for targeting users with egg freezing and donation advertisements.

Getting audience identities "right" is therefore a fraught task that is always already bound up with sociocultural, economic, and cultural discriminations. But what if the quest to get user identity "right" is the wrong way of looking at things? Carina Westling argues that anticipating audiences via their demographics and identity markers is not the only way that platforms can understand their users.[49] She proposes that platforms should understand web users not through their positionalities as identity-marked, individual *agents*, but instead through their collective, dynamic *agencies*—groups of users that move through and make decisions in a (digital) space. This approach involves platforms understanding their audiences as dynamic flows rather than demographically valued objects and managing or valuing them as such. Computationally, this way of modeling audiences is possible, but commercially would require a total overhaul of the data-for-services web.[50]

Visit the web version of this article to view interactive content.

Beverley Skeggs - All Data is Credit Data #TradingFaces

How (Not) to Target Web Users: Thoughts for Best Practice

Algorithmic targeting is never the simple computational process it might first seem to be: it is always bound up with ethically weighted sociocultural, political, and economic considerations. This is compounded by the fact that globally, there are still very few legislative measures designed to truly regulate targeting and protect users from both individual and collective pattern discriminations or systemic bias. Although this is changing, it is still very much up to developers to think carefully and ethically about who they profile, how, and for what reasons. To conclude, I offer some tentative thoughts for best practice on how (not) to target. What would you add?

- Think carefully about who you are targeting and why. What attributes are you assuming your target audience has, and why are you assuming this?
- Know why you are collecting data sets and what you will do with them: avoid collecting additional information just because your system is capable of it.
- Do not blindly trust the modeling sets you have access to: question if they are as representative as they claim or appear to be.
- Targeting is not just about data: it's about content and representation too! Consider the messages implied in what you are targeting.
- Target by content or item rather than user.
- Target by behavior rather than body.
- Avoid creating complex cookie notices and privacy policies: instead, think critically about how you can alleviate the burden of data responsibility from the user.
- How can you dispel any myths that may lead users to "algorithmic disillusionment"? What should your users know about your system's algorithmic power, or lack of it?
- Don't assume that there is an "ideal user": historic and existing sociocultural inequality means the ideal user is most often assumed to be white, cis-gendered male, heterosexual, middle class.
- What kinds of relevance should you be designing for: personal, collective, democratic, diverse, other? Should counter-relevance be considered?
- The legislative landscape on targeting is still in its infancy: should your systems be designed in compliance with the law, or with higher standards of best practice?
- Do you really need identity profiling at all? Would modeling audience flows or session-based targeting work instead?

Appendix: Brief Explanations of Selected Technological Terms and Processes

1. The HTTP cookie is "a way of storing information on the user's computer about a transaction between a user and a server that can be retrieved at a later date by the server."[51] Cookie tracking works by storing this text file on a user's computer and sending it to either third- or first-party cookie trackers, who then use this data to attribute characteristics to the user in the form of demographic profiling and other profiling mechanisms. It is important to note that cookies ultimately only capture information that is decipherable through abstracted correlation and "pattern recognition."[52] These abstract identifiers are then *translated back* into marketing demographic profiles by data brokers: computational referents of correlational and networked positionality are converted into "man," "woman," and so on by complex pre- and post-cookie data categorizations. It is the rendering of cookie data into "traditional social parameters" that makes cookie tracking so common and profitable.[53]
2. Cookieless tracking refers to identifying and anticipating users through technologies alternative to the HTTP cookie. Common types of tracking have included Flash and canvas "fingerprinting," which are seen as preferential to cookie tracking since fewer web users are aware of these technologies and they cannot be easily deleted.[54] Third-party cookie aggregation is set to be banned by Google and other platforms by 2022. This is partially in response to privacy concerns: however, as the Electronic Frontier Foundation notes, Google is essentially replacing third-party cookie tracking with a new experimental tracking system that still works by "sorting their users into groups based on behavior, then sharing group labels with third-party trackers and advertisers around the web," but in ways that users cannot necessarily know about or consent to.[55]
3. Session-based targeting refers to some recommender systems (found in software such as online music players) designed to suggest personalized content within a short and specific time-based period of user engagement. Models such as this tend to focus on the *content* of what is being personalized, combined with the short-term, context-based decisions of the user, to infer items of relevance.
4. Real-time bidding is a process used to display personalized advertising on web pages across the internet. Real-time bidding works as an auction process, wherein advertisers bid for an "impression" (ad space) seen by a particular user on the website they are visiting. Bidding, as the name suggests, is in real time and is largely fought and won using a combination of user profiling and content review of the

website hosting the advertisement. Almost all online search advertising is sold through this process because it allows marketers, brands, and businesses to deliver personalized ads based on user demographics to the same user across sites, devices, and platforms.

Bibliography

Abbate, Janet. "Privatizing the Internet: Competing Visions and Chaotic Events,1987–1995." *IEEE Annuals of the History of Computing* 32, no. 1 (2010): 10–22.

Apprich, Clemens, Wendy Hui Kyong Chun, Florian Cramer, and Hito Steyerl. *Pattern Discrimination.* Minneapolis: University of Minnesota Press, 2018.

Bassett, Caroline. "Identity Theft." In *Sensorium: Embodied Experience, Technology and Contemporary Art, edited by* Caroline A. Jones. Cambridge, MA: MIT Press, 2006.

Barker, Alex. "'Cookie apocalypse' forces profound changes in online advertising." *Financial Times,* February 25, 2020.

BBC. "Facebook to Show Who Buys Political Ads." *BBC News, October 28, 2017.*

Bivens, Rena, and Oliver L. Haimson. "Baking Gender into Social Media Design: How Platforms Shape Categories for Users and Advertisers." *Social Media + Society* 2, no. 4 (2016): 1–12.

Bolin, Göran, and Jonas Andersson Schwarz. "Heuristics of the Algorithm: Big Data, User Interpretation and Institutional Translation." *Big Data & Society* 2, no. 2 (2015).

Browne, Simone. *Dark Matters*. Durham, NC: Duke University Press, 2015.

Bucher, Taina. "The Algorithmic Imaginary: Exploring the Ordinary Affects of Facebook Algorithms." *Information, Communication & Society* 20, no. 1 (2016): 30–44.

Business Insider. "Facebook Ad Revenue in 2020 Will Grow 4.9% Despite the Growing Number of Brands Pulling Campaigns." June 23, 2020.

Cheney-Lippold, John. *We Are Data: Algorithms and the Making of Our Digital Selves.* New York: New York University Press, 2017.

Curran, James, and John Seaton. *Power without Responsibility: Press, Broadcasting and the Internet in Britain: Press and Broadcasting in Britain*. London: Routledge, 2010.

Cyphers, Bennett. "Google Is Testing Its Controversial New Ad Targeting Tech in Millions of Browers." *Electronic Frontier Foundation*, March 30, 2021.

Egbert, Simon, and Matthias Leese. *Criminal Futures*. London: Routledge, 2020.

Eubanks, Virginia. *Automating Inequality*. New York: St. Martin's Press, 2017.

Facebook. "Ad Library." Accessed July 12, 2019.

Facebook Newsroom. "Introducing Anonymous Login and an Updated Facebook Login." April 30, 2014.

Finn, Ed. *What Algorithms Want: Imagination in the Age of Computing.* Cambridge, MA: MIT Press, 2017.

Gates, Bill. *The Road Ahead*. New York: Viking, 1995.

Google. "An Update on Our Political Ads Policy," n.d. Accessed November 20, 2019.

Greenfield, Peter. "The Cambridge Analytica Files: The Story So Far." *Guardian*, March 25, 2018.

Hagel, John, and Arthur Armstrong. *Net Gain: Expanding Markets through Virtual Communities*. Boston: Harvard Business School Press, 1997.

Henderson, Monica Jean, Leslie Regan Shade, and Katie Mackinnon. "Every Click You Make: Algorithmic Literacy and the Digital Lives of Adults." *AoIR Selected Papers of Internet Research* (2020, October).

Jarrett, Kylie. "A Database of Intention?" In *Society of the Query Reader: Reflections on Web Search*, edited by René König and Miriam Rasch, 16–29. Amsterdam: Institute of Network Cultures, 2014.

Kant, Tanya. *Making It Personal: Algorithmic Personalization, Identity and Everyday Life.* New York: Oxford University Press, 2020.

Kelion, Leo. "How to Handle the Flood of GDPR Privacy Updates." *BBC News*, April 28, 2018.

Kitchin, Rob, and Martin Dodge. *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press, 2011.

Ludewig, Malte, Noemi Mauro, Sara Latifi, and Dietmar Jannach. "Empirical Analysis of Session-Based Recommendation Algorithms." *User Modeling and User-Adapted Interaction* 31 (2021): 149–81.

Mahdawi, Arwa. "Targeted ads are one of the world's most destructive trends. Here's why." *The Guardian,* November 5, 2019.

Nikiforakis, Nick, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giavanni Vigna. "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting." *2013 IEEE Symposium on Security and Privacy* (2013): 541–55.

Noble, Safiya Umoja. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press, 2018.

Ofcom. "Adults' Media Use & Attitudes report 2020." Accessed May 17, 2021.

O'Neil, Cathy. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy.* London: Penguin, 2016.

Pasek, Anne, Rena Bivens, and Mél Hogan. "Data Segregation and Algorithmic Amplification: A Conversation with Wendy Hui Kyong Chun." *Canadian Journal of Communication* 44, no. 3 (2019): 455–69.

Pariser, Eli. *The Filter Bubble: What the Internet Is Hiding from You.* London: Penguin, 2011.

Peacock, Sylvia. "How Web Tracking Changes User Agency in the Age of Big Data: The Used User." *Big Data & Society* 2, no. 1 (2014).

Rheingold, Howard. *The Virtual Community: Homesteading on the Electronic Frontier.* Cambridge, MA: MIT Press, 1996.

Reed, Elizabeth, and Tanya Kant. "'One Donor Egg and A Dollop of Love': ART and De-queering Genealogies in Facebook Targeted Advertising." *Feminist Theory* (Forthcoming).

Skeggs, Beverley. *You Are Being Tracked, Valued and Sold: An Analysis of Digital Inequalities,* 2017. Lecture, Filmed September 2017 at the London School of Economics, MP4, run time 1:26:42.

Tamò Larrieux, Aurelia, Eduard Fosch Villaronga, Shruthi Velidi, Salome Viljoen, Christoph Lutz, and Moritz Büchi. "Perceptions of Algorithmic Profiling on Facebook and Their Social Implications." *AoIR Selected Papers of Internet Research* (2020, October).

Taylor, T. L. *Watch Me Play: Twitch and the Rise of Game Live Streaming*. Princeton, NJ: Princeton University Press, 2018.

Turow, Joseph, Michael Hennesy, and Nora Draper. "*The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*." Preprint, submitted June 26, 2015. SSRN paper 2820060.

Van Couvering, Elizabeth. "Is Relevance Relevant? Market, Science, and War: Discourses of Search Engine Quality." *Journal of Computer Mediated Communication* 12, no. 3 (2007): 866–87.

Wang, Jackie. *Carceral Capitalism*. Cambridge, MA: MIT Press, 2020.

Wang, Jun, Weinan Zhang, and Shuai Yuan. "Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting." *Foundations and Trends in Information Retrieval* 11, no. 4–5 (2017): 297–435.

Westling, Carina E. I. *Immersion and Participation in Punchdrunk's Theatrical Worlds*. London: Bloomsbury, 2020.

Wong, Julia Carrie. "'It might work too well': the dark art of political advertising online." *The Guardian,* March 19, 2018.

Zuckerman, Ethan. "The Internet's Original Sin." *Atlantic,* August 14, 2014.

Press Play ▶ NPR talks with Frank O'Brien, CEO of a marketing software company Five Tier about being tracked by online advertisers.

Visit the web version of this article to view interactive content.

Footnotes

1. "Facebook Ad Revenue in 2020 Will Grow 4.9%," *Business Insider,* June 23, 2020. ↩

2. John Cheney-Lippold, *We Are Data* (New York: New York University Press, 2017), 4. ↩
3. Caroline Bassett, "Identity Theft," in *Sensorium: Embodied Experience, Technology and Contemporary Art,* ed. Caroline A. Jones (Cambridge: MIT Press, 2006), 155. ↩
4. T. L. Taylor, *Watch Me Play: Twitch and the Rise of Game Live Streaming* (Princeton, NJ: Princeton University Press, 2018). ↩
5. Beverley Skeggs, *You Are Being Tracked, Valued and Sold: An Analysis of Digital Inequalities*, London School of Economics (September 2017). ↩
6. Safiya Umoja Noble, *Algorithms of Oppression* (New York: New York University Press, 2018). ↩
7. Cathy O'Neil, *Weapons of Math Destruction* (London: Penguin, 2016). ↩
8. This timeline centers largely on developments that have affected European (and to a lesser extent US) web users, and cannot include all historically significant targeting events, even in this locality. ↩
9. For work in these fields see Jackie Wang, *Carceral Capitalism* (Cambridge, MA: MIT Press, 2020); Virginia Eubanks, *Automating Inequality* (New York: St. Martin's Press, 2017); Simon Egbert and Matthias Leese, *Criminal Futures* (London: Routledge, 2020); Simone Browne, *Dark Matters* (Durham: Duke University Press, 2015)*;* and Rob Kitchin and Martin Dodge, *Code/space* (Cambridge, MA: MIT Press, 2011). ↩
10. Janet Abbate, "Privatizing the Internet: Competing Visions and Chaotic Events, 1987–1995," *IEEE Annuals of the History of Computing* 32 (2010): 10, 10–22. ↩
11. Invented by Tim Berners Lee, the World Wide Web is a hyperlinked information system that can be used to access the internet. ↩
12. Howard Rheingold, *The Virtual Community* (Cambridge, MA: MIT Press, 1996). ↩
13. Bill Gates, *The Road Ahead* (New York: Viking, 1995); John Hagel and Arthur Armstrong, *Net Gain* (Boston: Harvard Business School Press, 1997). ↩
14. See section 1 of the appendix. ↩

15. Sylvia Peacock, "How Web Tracking Changes User Agency in the Age of Big Data: The Used User," *Big Data & Society* 2, no. 1 (2014): 6. ↩
16. James Curran and John Seaton, *Power Without Responsibility* (London: Routledge, 2010). ↩
17. Ethan Zuckerman, "The Internet's Original Sin," *Atlantic*, August 14, 2014. ↩
18. See section 4 of the appendix. ↩
19. Peacock, "How Web Tracking Changes User Agency." ↩
20. Nick Nikiforakis *et al.,* "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting," *2013 IEEE Symposium on Security and Privacy* (2013): 541–55. ↩
21. "Introducing Anonymous Login," *Facebook Newsroom,* April 30, 2014. ↩
22. Peter Greenfield, "The Cambridge Analytica Files: The Story So Far," *Guardian*, March 25, 2018. ↩
23. Alex Barker, "'Cookie apocalypse' forces profound changes in online advertising," *Financial Times,* February 26, 2020. ↩
24. Kyle Jarrett, "A Database of Intention?," in *Society of the Query Reader: Reflections on Web Search*, ed. René König and Miriam Rasch (Amsterdam: Institute of Network Cultures, 2014), 16–29; Cheney-Lippold, *We Are Data*. ↩
25. Ofcom, "Adults' Media Use & Attitudes Report 2020," accessed May 17, 2021. ↩
26. Ofcom, "Adults' Media Use." ↩
27. Joseph Turow, Michael Hennessy, and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," Preprint, submitted June 26, 2015, SSRN paper 2820060. ↩
28. Ofcom, "Adults' Media Use." ↩
29. Tanya Kant, *Making It Personal: Algorithmic Personalization, Identity, and Everyday Life* (New York: Oxford University Press). ↩
30. Kant, *Making It Personal,* 99. All study participants were assigned pseudonyms to protect their privacy. ↩

31. Julia Carrie Wong, "'It might work too well': the dark art of political advertising online," *The Guardian* (March 19, 2018); Arwa Mahdawi, "Targeted ads are one of the world's most destructive trends. Here's why," *The Guardian* (November 5, 2019). ↩
32. Ofcom, "Adults' Media Use." ↩
33. Kant, *Making It Personal,* 182. ↩
34. Kant, *Making It Personal,* 158–97. ↩
35. Taina Bucher, "The Algorithmic Imaginary: Exploring the Ordinary Affects of Facebook Algorithms," *Information, Communication & Society* 20, no. 1 (2016): 30–44; Ed Finn, *What Algorithms Want: Imagination in the Age of Computing* (Cambridge, MA: MIT Press, 2017); and Kant, *Making It Personal.* ↩
36. Aurelia Tamò Larrieux *et al.*, "Perceptions of Algorithmic Profiling on Facebook and Their Social Implications," *AoIR Selected Papers of Internet Research* 2020 (October). ↩
37. Leo Kelion, "How to Handle the Flood of GDPR Updates," *BBC News* (April 28, 2018). ↩
38. Monica Jean Henderson, Leslie Regan Shade, and Katie Mackinnon, "Every Click You Make: Algorithmic Literacy and the Digital Lives of Young Adults," *AoIR Selected Papers of Internet Research* 2020 (October). ↩
39. Johnathan Stempel, "Facebook Sued for Age, Gender Bias in Financial Services Ads," *Reuters,* October 31, 2019. ↩
40. Google, "An Update on Our Political Ads Policy," n.d., accessed November 20, 2019. ↩
41. Clemens Apprich *et al., Pattern Discrimination* (Minneapolis: University of Minnesota Press, 2018). ↩
42. Apprich *et al., Pattern Discrimination*, x. ↩
43. Wendy Chun quoted in Anne Pasek, Rena Bivens, and Mél Hogan, "Data Segregation and Algorithmic Amplification: A Conversation with Wendy Hui Kyong Chun," *Canadian Journal of Communication* 44, no. 3 (2019): 467, 455–69. ↩

44. Noble, *Algorithms of Oppression.* ↩

45. Elizabeth Van Couvering, "Is Relevance Relevant? Market, Science, and War: Discourses of Search Engine Quality," *Journal of Computer-Mediated Communication 12, no. 3* (2007): 866–87; Eli Pariser, *The Filter Bubble* (London: Penguin, 2011); Malte Ludewig et al., "Empirical Analysis of Session-Based Recommendation Algorithms," *User Model User-Adapted Interaction 31* (2021): 149–81. ↩

46. Elizabeth Reed and Tanya Kant, "'One Donor Egg and A Dollop of Love': ART and De-queering Genealogies in Facebook Targeted Advertising," *Feminist Theory* (forthcoming). ↩

47. Rena Bivens and Oliver Haimson, "Baking Gender into Social Media Design: How Platforms Shape Categories for Users and Advertisers," *Social Media + Society* 2, no. 4 (2016): 1–12. ↩

48. Bivens and Haimson "Baking Gender," 7. ↩

49. Carina Westling, *Immersion and Participation in Punchdrunk's Theatrical Worlds* (London: Bloomsbury, 2020). ↩

50. Session-based recommenders use comparable models: see section 3 of the appendix. ↩

51. Peacock, "How Web Tracking Changes User Agency," 14. ↩

52. Göran Bolin and Jonas Andersson Schwarz, "Heuristics of the Algorithm: Big Data, User Interpretation and Institutional Translation," *Big Data & Society* 2, no. 2 (2015). https://doi.org/10.1177/2053951715608406. ↩

53. Bolin and Schwarz, "Heuristics of the Algorithm," 1. ↩

54. Jun Wang, Weinan Zhang, and Shuai Yuan, "Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting," *Foundations and Trends in Information Retrieval* 11, no. 4–5 (2017): 297–435. ↩

55. Bennett Cyphers, "Google Is Testing Its Controversial New Ad Targeting Tech in Millions of Browers," *Electronic Frontier Foundation,* March 30, 2021. ↩